IN THE SPECIFICATION

Paragraph 0072, as listed in the published application (number US 2002/0186848) is sought to be rewritten as follows:

[0072] It is suggested that, to achieve better security in hop-by-hop routing mode, every two consecutive cipher versions of the message be delivered with a time gap of few milliseconds. No specific time gap is required in source routing mode. Source routing is more preferable as it fully ensures that all the cipher versions do not meet at a single router before their destination. In source routing, the paths are so selected that they all ~~don~~ do not meet concurrently at a single router before destination. An attacker who wants to obtain the original message from a single encrypted version of it has to try different possible values of t, the blinding number. A multiplicative inverse has to be computed for each e.sub.1+t or e.sub.2+t, and an exponential modular operation needs to be performed with each of these as the decrypting exponent like in RSA attacks. One of the exponents will yield the original message. But the attacker never knows as to which particular t value yields the right message. The searching range of t for an attacker is (-min(e.sub.1, e.sub.2) to phi). Since the order of phi is same as n, the attacker has to perform nearly n mathematical operations where as RSA system requires only square-root(n) operations. Moreover, the mathematical operations are more expensive than the modular operations of the RSA. Therefore, the security factor of this cryptographic system over RSA is more than square-root(n). For example if a 512 bit key is used for encryption, breaking the ~~cipbertext~~ ciphertext of this cryptographic system takes more than 2.sup.256 times the period as required by RSA.